PD 686-037

SeaWinds Experiment

Systems Safety Requirements

July 1994

JPL
Jet Propulsion Laboratory

PD 686-037

SeaWinds Experiment

Systems Safety Requirements

Prepared by: _____
J. S. Michel
Systems Safety Engineer

Approved by: _____
A. P. Bowman, Acting Manager
Systems Safety Office

Approved by: _____
M.C. Trummel, Manager
Product Assurance

Approved by: _____
J. E. Graf, Manager
SeaWinds Project

July 1994

Jet Propulsion Laboratory
California Institute of Technology

SEAWINDS SYSTEMS SAFETY REQUIREMENTS

DOCUMENT LOG

Date	Revision No.	Notes
		BASIC ISSUE

SEAWINDS SYSTEMS SAFETY REQUIREMENTS

FOREWARD

The JPL Standard for Systems Safety (JPL D-560) has been tailored and provided for the SeaWinds Project in the form of this document. It is specifically applicable to SeaWinds Project's contracts and contractor activities.

JPL 'in-house' activities and JPL personnel must comply with JPL D-560. Sections were removed from the standard because they were determined not applicable to the SeaWinds Project's Contractors. The following assumptions were the basis to omit specific requirements which appear not applicable to SeaWinds Project hardware:

1) No ionizing radiation;
2) No solid propellant motors;
3) No pressure vessels;
4) Not be launched or recovered on the STS (Space Shuttle);
5) No liquid propellant systems;
6) No pressurized systems;
7) No cryogenic systems; and
8) Contractor not involved with Launch Operations.

If these assumptions are incorrect or change, write to the following address or fax and request the applicable Safety Requirements:

Jet Propulsion Laboratory
Attention: Scott Michel
M/S 301-375
4800 Oak Grove Drive
Pasadena, CA 91109
FAX: (818) 393-4497

To receive copies of the Facility Safety Survey, Operations Safety Survey, Transportation Safety Survey, and/or ESD Survey, send a request to the above.

Contractor may use equivalent existing systems and processes after review and approval by JPL.

These SeaWinds Requirements were written specifically for the SeaWinds Project and are not applicable to any other project. They are based upon an understanding of the level of risk which the SeaWinds Project Manager is willing to accept for the Project.

SEAWINDS SYSTEMS SAFETY REQUIREMENTS

ACRONYM LIST

AHSE	Assembly, Handling and Shipping Equipment
CDRL	Contract Data Requirements List
D	Document
dB	Decibel
DOT	Department of Transportation
ELV	Expendable Launch Vehicle
ESD	Electrostatic Discharge
FED-STD	Federal Standard
GSE	Ground Support Equipment
JPL	Jet Propulsion Laboratory
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
mW/cm^2	MilliWatts per Square Centimeter
NEIs	Non-Explosive Initiators
PD	Project Document (SeaWinds Document)
P/FR	Problem/Failure Report
psi	Pounds per Square Inch
RF	Radio Frequency
RMS	Root Mean Square
SCI	SeaWinds Critical Item
V	Volts
VAC	Volts Alternating Current
VDC	Volts Direct Current

SEAWINDS SYSTEMS SAFETY REQUIREMENTS

CONTENTS

SEAWINDS SYSTEMS SAFETY REQUIREMENTS

CONTENTS (Cont'd)

CONTENTS (Cont'd)

CONTENTS (Cont'd)

SECTION 1

POLICY AND ORGANIZATION

1.1 SCOPE

This SeaWinds Systems Safety Requirements document is designed to assist managers, designers, engineers, and technicians in implementing safety requirements in their projects.

1.2 APPLICABILITY

This requirements document is applicable to the JPL SeaWinds Project and its Contractors. JPL and JPL personnel must comply with JPL D-560. The application of specific requirements contained within this document are governed by the following criteria:

(1) The hardware shall meet personnel safety requirements (ref. JPL D-8966).

(2) The SeaWinds' hardware shall meet all safety requirements for hardware protection and thus shall comply with this document in its entirety. Any deviations require the preparation and approval of a waiver (Ref. Para. 1.4).

(3) Hardware valued above $100,000 shall be provided hardware protection by performing Facility and Operations Safety Surveys. Hardware protective measures to be required are at the discretion of the cognizant manager who has ultimate authority over and responsibility for the hardware.

1.3 POLICY AND IMPLEMENTATION

The Jet Propulsion Laboratory policy requires safety for all personnel and equipment in consonance with project achievement.

The Contractor shall conform with all local, State, Federal, and Foreign regulations regarding safety. Because there are "experimental" clauses, such regulations have little constraint on experimental designs but closely control nonexperimental ground support equipment.

1.3.1 Safety Responsibility

It is the responsibility of the hardware suppliers to provide all information necessary to support the safety certification as specified in the Contract Data Requirements List (CDRL).

1.3.2 Safety Steering Committee

1.3.2.1 Safety Steering Committee. A Safety Steering Committee or equivalent shall be established. The membership shall involve those Managers having line safety responsibility for any operations or activities which include design, assembly, test, and transportation of both flight and ground hardware.

A Manager may appoint an alternate to represent him/her on the Committee if he/she so desires, but the Manager's safety responsibility cannot be delegated. The degree of the Manager's participation in the Committee should be commensurate with the hazards associated with the activity for which he/she is responsible.

The Contractor Project Manager shall be the chairman and, with the Contractor Systems Safety Engineer, shall be permanent members of the Committee. Other membership shall be comprised of the Managers having specific responsibilities for design, test, or operation of the Hardware and any special consultants.

1.3.2.2 Committee Responsibilities. The Safety Steering Committee shall carry out the following duties:

(1) Review and approve the applicability of safety requirements for the project.

(2) Perform a hazard review of the flight hardware, software, and GSE design.

(3) Evaluate techniques for minimizing or safely accommodating the hazards that cannot be eliminated.

(4) Review hazard reports and safety packages prepared for transmittal to outside agencies such as launch agency, etc.

(5) Evaluate appropriate test and operations schedules and sequences to assure maximum personnel and equipment safety.

(6) Review design changes which have safety implications and concur that changes are acceptable from a safety viewpoint.

1.3.2.3 Frequency of Meetings. Meetings shall be held until the review of all safety concerns of the project are complete and appropriate actions are completed. If the design has no impact on the safety of the personnel or hardware, then only a single review is required to ascertain that no hazards exist.

1.3.3 Documentation

The specific safety requirements applicable to each program or project shall be defined in the Safety Plan (Section 1.3.3.1). Ground and flight hazards shall be identified on Hazard Reports (Section 1.3.3.2).

1.3.3.1 Safety Plan. A Safety Plan is required from each JPL contractor and subcontractor. Safety Plans for high level assemblies such as projects and systems shall cover any sub-assemblies or lower level items which they contain.

The Safety Plan shall assure adequate safety to personnel, flight hardware, and ground support equipment. The safety considerations shall include assembly, inspection, handling (including shipping and transportation), test, and operations being or to be conducted in all facilities (contractor, subcontractor, JPL, university, or others). In general, the Safety Plan, as appropriate, shall include: (1) 1.0 Introduction; (2) 2.0 Applicable Documents; (3) 3.0 System Safety Program; (4) 3.1 System Safety Organization; (5) 3.2 System Safety Schedules; (6) 3.3 System Safety Requirements; (7) 3.4 Hazard Analyses; (8) 3.5 System Safety Data; (9) 3.6 Hardware Protection; (10) 3.7 Software Safety; (11) 4.0 System Safety Assurance; (12) 4.1 Training; (13) 4.2 Audit Program; (14) 4.3 Mishap Reporting and Investigation; and (15) 4.4 System Safety Interfaces.

1.3.3.2 Hazard Report. For missions utilizing expendable launch vehicles, a hazard report form as agreed to by JPL and the contractor shall be generated for each hazard.

The hazard reports shall be collected and, together with relevant safety back-up data, assembled into a Safety Data Package. After compiling the hazard reports, the contractor shall send the Safety Data Package to JPL (SeaWinds Systems Safety Engineer). Items that should be listed in the document include, but is not limited to: (1) Flammables in hazardous quantity; (2) Toxic materials (beryllium metal and dust, solvents, mercury, etc.); (3) Voltages above 30 VDC or 30 VAC RMS (50 V if equipment is used only at JPL); (4) Energy storage devices (springs, tensioned cables, etc.); (5) Batteries; (6) Asphyxiants (nitrogen, helium, argon, neon, xenon, etc.); (7) Corrosives; (8) Rotating equipment; (9) Ionizing and nonionizing radiation sources (RF, laser, x-ray, microwave, nuclear, etc.); and (10) High temperatures.

1.3.3.3 Drawings and Documentation. The following safety-related information shall be included in engineering documentation:

1.3.3.3.1 Hazardous Items. Drawings or other design documentation for items or assemblies which present potential or actual hazards to personnel or equipment shall bear appropriate notification of those hazards.

1.3.3.3.2 Items Subject to Degradation. Design documentation and procedures for items which are subject to degradation stemming from personnel, other equipment, or environmental factors shall bear appropriate notification of these vulnerabilities.

1.3.3.4 Safety Requirement Verification. Activities performed to satisfy a safety requirement shall be documented.

1.3.3.5 Discrepancy Reporting. Problems, failures, or discrepancies which may have a potential impact on safety of personnel or hardware shall be recorded using existing reporting systems and reported to cognizant engineering or Quality Assurance personnel. This action shall not be used as the basis for any punitive action. The Contractor's Technical Manager and the JPL SeaWinds Systems Safety Engineer shall be notified verbally as soon as possible and shall receive a copy of the initial written report.

1.3.3.6 Reviews. Safety shall be included on the agenda of all formal and informal reviews associated with SeaWinds at all levels (design, delivery, test readiness, preship, etc.). The safety material included shall be tailored to the nature of the review and the maturity of the project. In the case where there are no safety implications involved, a statement to that effect shall be included in the review package.

1.3.4 Procurement

The Contractor shall ensure that appropriate safety requirements are included in all subcontracts. A written Safety Plan to be approved by JPL is required (Reference CDRL).

1.4 WAIVERS AND EXCEPTIONS

This SeaWinds Systems Safety Requirements document may be waived/excepted when alternate methods are employed to achieve the required protection and the risk of injury to personnel or loss of or damage to hardware is acceptably low.

1.5 DEFINITIONS

The following definitions are established to provide a common base of interpretation of requirements within this document. Due to the broad application of this document, it is recognized that the definitions in use on individual projects and by other institutions may vary in actual usage.

1.5.1 Project

Project is any project, program, experiment, task, or activity for which the institution (JPL or JPL Contractor) has responsibility to an outside agency for its successful accomplishment.

1.5.2 Project Manager

The Project Manager refers to that individual who has the institutional responsibility (JPL or JPL Contractor) to an outside agency for successful accomplishment of a project.

1.5.3 SeaWinds Critical Items

SeaWinds Critical Items (SCI's) are that critical hardware, software, test, and/or handling equipment, including fixtures or ground support equipment which, if damaged or lost, would:

(1) Jeopardize the successful accomplishment of the project, or;

(2) Result in a substantial cost increase or schedule impact to the project, or;

(3) Result in an impact of $100k or greater per item regardless of program/experiment.

Included under this category are the following:

1.5.3.1 Flight Hardware. Flight hardware refers to any hardware/equipment that leaves the surface of the earth.

1.5.3.2 Flight-Critical Hardware. Flight-critical hardware includes all flight hardware and project-critical hardware.

1.5.3.3 Project-Critical Hardware. Project-critical hardware or equipment refers to those items which, if damaged or lost, would cause a major cost or schedule impact to the project (i.e., if the cognizant hardware organization would require significant additional funds or schedule time to meet the original commitment), or, if not replaced, would jeopardize the successful accomplishment of the mission or project. It may include any of the ground support equipment identified below which are critical to the mission or project. Functional replicas of flight equipment that are not intended for flight, such as engineering models, may also be designated Project-Critical if they provide a critical ground test capability, either before or after launch.

1.5.3.4 Ground Support Equipment. Ground Support Equipment (GSE) is defined as any equipment, electrical or mechanical, which is used to assemble, test, handle, or launch the flight equipment. It includes, but is not limited to, assembly and handling fixtures, system test complex and launch complex equipment, and transportation equipment. This may include equipment which does not directly interface to the flight equipment. Assembly, Handling, and Shipping Equipment (AHSE) is included under the broad definition of GSE.

1.5.4 Safety Critical

Safety critical refers to equipment, software, or functions which, if nonfunctional, inoperative, or incorrectly performed, could injure personnel or damage equipment.

1.5.4.1 Hazardous Operation . A hazardous operation is any process or series of functions in which one or more of the following conditions are present:

(1) Energy is involved and loss of control could result in injury to personnel or damage to equipment.

(2) A significant change from ambient condition shall occur; e.g. increase or decrease of pressure, temperature, or work-place oxygen content.

(3) Presence of hazardous materials which presents the potential for personnel exposure.

1.5.5 System

A system refers to the complete set of subsystems and support equipment which shall perform the mission or project.

1.5.6 Subsystem

A subsystem refers to the first major division of a system, generally divided into functional elements.

1.5.7 Assembly

An assembly refers to the first major division of a subsystem.

1.5.8 Experiment

Refer to "project."

1.5.9 Environmental Test

Environmental test refers to the intentional application of any environment which has the potential of damaging the hardware, regardless of the location of the test facility or the phase of the hardware cycle. This specifically includes environments imposed for processing, as well as those imposed for qualification or acceptance testing purposes.

1.5.10 Catastrophic Hazard

A hazard which can result in the potential for a disabling or fatal personnel injury, or loss of facilities or equipment.

1.5.11 Critical Hazard

A hazard which can result in damage to equipment, a nondisabling personnel injury, or the unscheduled use of safing procedures that affect operators of a JPL payload.

1.5.12 Structure

Parts and assemblies which sustain loads by providing physical support and/or containment.

1.5.12.1 Failure. The condition under which the structure or any part thereof can no longer perform its intended structural function. Such a condition may be caused by instability, rupture, or excessive deformation.

1.5.12.2 Limit Loads or Stresses. Limit loads or stresses represent the maximum physical loads or stresses the structure is expected to experience under specified conditions of operation or use.

1.5.12.3 Structure Classification. Primary Structure is any structural element supporting more than 20 kg of mass.

1.5.12.4 Ultimate Factor of Safety. The ultimate factor of safety is a multiplying factor applied to a limit load or stress to obtain the load at which there shall be no structural failure.

1.5.12.5 Ultimate Load or Stress. The ultimate load or stress is the maximum load or stress a structure can sustain without failure.

1.5.12.6 Yield Factor of Safety. The yield factor of safety is a multiplying factor applied to the limit load to obtain the load at which there shall be no general yielding of the structure. This does not apply to local yielding at stress concentrations, etc.

1.5.12.7 Rated Load. Rated load is the maximum load that may be applied at any given time.

1.5.13 Ordnance

The term "electroexplosive ordnance" includes, but is not limited to, ignitors, explosives, pyrotechnics, and electroexplosive devices that are initiated electrically.

1.5.13.1 Category A. Ordnance devices which may cause injury or death to personnel or damage to facility property by the expenditure of their own energy, or by initiating a chain of events, shall be classified as Category A devices. Damage to project equipment only is not sufficient grounds for classifying a device as Category A.

1.5.13.2 Category B. Ordnance devices which are not classified as Category A shall be classified as Category B.

1.6 APPLICABLE DOCUMENTS

The following documents of the issue in effect at the time of release of this document form a part of this requirements document as specified herein. Conflict between applicable documents and this document shall be referred to the SeaWinds Systems Safety Engineer for resolution.

JPL DOCUMENTS

D-560 JPL Standard For Systems Safety
(Applicable only to JPL and JPL personnel)

PD 686-014 SeaWinds Instrument Software Management Requirements

FEDERAL DOCUMENTS

FED-STD 209 Clean Room and Work Station Requirements, Controlled Environment

MILITARY DOCUMENTS

MIL-STD 1576 Electroexplosive Subsystem Safety Requirements and Test Methods For Space Systems

MIL-HDBK 5 Metallic Materials And Elements For Aerospace Vehicle Structures

JPL DRAWINGS

10025963-1 Proof-test Label/AHSE
(See Appendix A)

1.7 REFERENCE DOCUMENTS

The following document of the issue in effect at the time of release of this document is included for reference purposes only. Conflict between the referenced document and this document shall be referred to the SeaWinds Systems Safety Engineer for resolution.

JPL DOCUMENTS

D-8966 JPL Standard for Flight Instrument Classifications and Product Assurance Requirements

SECTION 2

FLIGHT EQUIPMENT DESIGN REQUIREMENTS

[--- Unable To Translate Graphic ---]

2.1 GENERAL

Edges of flight equipment accessible to personnel shall be designed so as to preclude injury during handling and testing.

2.2 ELECTROMECHANICAL DEVICES

For spacecraft which will be launched on an ELV, electromechanical devices (including NEIs) which are used for such purposes as structure deployment or actuation release mechanisms shall be evaluated to determine the possibility of damage to equipment or injury to personnel in the case of inadvertent activation. If damage or injury is determined to be possible, the device(s) shall be controlled in a manner similar to Category "A" ordnance devices. At least two independent serial actions shall be required prior to the activation of the device in flight and at least three independent serial actions for activation on the ground.

2.3 ELECTRICAL SYSTEMS

The following criteria govern safety design requirements for electrical power subsystems.

2.3.1 Explosion-Proofing

The flight equipment shall be designed and constructed so that energizing or operating an electrical circuit planned to be energized during prelaunch, ascent, or descent activities in the presence of flammable vapors cannot initiate an explosion or fire.

Special design consideration for explosion hazards shall be given to, but not be limited to, the following:

(1) Motors, mechanical contact switches, or other devices which may spark during use.

(2) Devices which incorporate items such as heated elements or open flame which develop temperatures high enough to ignite flammable vapors, dust, or other materials.

(3) Devices which employ arcs or spark discharges in their operation or incorporate voltages in excess of 100 volts which could conceivably cause corona or sparks.

(4) Items or materials which could react chemically with oxidizing materials (such as propellants), causing high temperatures or fires.

(5) Items which can produce quantities of flammable vapors or flammable dust.

(6) Oxidation-prone metals, such as magnesium, sodium, etc.

(7) Devices which normally operate in a pulsed mode which may overheat if continuously powered (such as isolation-latching valves, stepper motors, motorized switches, etc.).

2.3.2 Connectors

Connectors shall be selected and configured to satisfy safety-related requirements.

2.3.2.1 Mismating. Positive mechanical methods such as connector type, size, keying, or pin configuration shall be used where practicable to prevent mismating or cross-connections of electrical connectors where improper assembly could result in a personnel hazard or equipment damage.

2.3.2.2 Parallel Power Pin Failure. The failure of one or more connector pins in a parallel power carrying configuration shall not generate hazardous temperatures in the remaining power carrying pin(s) at full-rated circuit load (see Section 2.3.1). The resulting voltage drop at the load shall not create a hazardous condition or cause a hazardous function to occur.

2.3.3 Lead Wires

The failure of one or more lead wires in a parallel power carrying configuration shall not generate hazardous temperatures in the remaining power carrying wire(s) at full-rated circuit load. The resulting voltage drop at the load shall not create a hazardous condition or cause a hazardous function to occur.

2.4 STRUCTURE

2.4.1 Structure Requirements

Primary structure shall be designed using materials with MIL-HDBK 5 type "A" values (99% probability and 95% confidence).

2.4.1.1 Ultimate Factor of Safety. Minimum analytical factor of safety for ELV flight hardware structures is 1.25 (More stringent requirements may be specified for structural members which are not verified by test).

2.4.1.2 Additional Factors. Additional factors shall be applied to the yield and ultimate factors of safety if analysis uncertainties exist in areas such as joints and fittings, etc.

2.4.1.3 Fracture-Critical Composite/Bonded Structures. For all fracture-critical composite/bonded components, only manufacturing processes and controls that are demonstrated to be reliable and consistent with established aerospace industry practices shall be used. Procedures for the prevention of damage resulting from handling, testing, or final assembly shall be implemented and approved.

All fracture-critical composite/bonded components shall be proof tested to at least 120 percent of the limit load. The proof test shall be conducted on the flight articles and may be accomplished at the component, assembly, or system level.

2.4.2 Ground Handling Attach Points

2.4.2.1 Flight Interfaces. Lifting and handling loads and load paths for equipment attaching to flight interface points shall be included in the analyses on the flight structures.

2.4.2.2 Special Attachment Provisions. Special GSE lifting and handling attachment provisions designed into the flight hardware shall be analyzed and/or tested to verify that the attachment points and load paths have the same margin of safety for ground handling as is required for the flight load paths.

2.5 MATERIALS

2.5.1 Materials and Processes Control Plan

A Materials and Processes Control Plan (Reference CDRL) shall be prepared that includes all of the safety requirements contained in Section 2.5. The Plan shall also specify all criteria, procedures, and controls necessary to satisfy these requirements.

2.5.2 Materials Requirements

All materials shall be evaluated for flammability characteristics.

All materials that are exposed to hazardous fluids shall be evaluated for compatibility with the fluid in their application. A hazardous fluid is any fluid that could chemically or physically degrade the system or cause an exothermic reaction.

When materials can be exposed to hazardous fluids by a credible single barrier failure, an engineering evaluation and analysis of test data shall be conducted to demonstrate the acceptability of the configuration.

The use of chemicals (such as mercury) which would create a toxicity problem or cause a hazard to flight hardware if released shall be adequately contained.

2.6 COMPUTER SYSTEMS

Safety shall be designed into computer systems from their inception.

2.6.1 Fault Tolerance

For the purposes of determining the safety fault tolerance of a system, a computer system (hardware/software combined) shall be considered as zero safety fault tolerant unless different computers (hardware and type) using independently developed software are used to control different inhibits to a hazardous function.

2.6.2 Hardware/Software Inhibits

Wherever practical, safety-critical functions shall include at least one noncomputer-controlled inhibit which will preclude the inadvertent occurrence of hazardous functions in the event of a computer hardware or software failure.

2.6.3 Software Design

The portions of the software relating to safety-critical functions should be modularized as much as possible so as to minimize and isolate interactions with other non-safety critical software functions in order to reduce the required analysis effort. Multiple software inhibits should be designed into the safety-critical module to preclude activation by other system software and to allow only authorized removal of inhibits under very specific and precisely planned conditions.

2.6.4 Software Hazard Analysis

A software hazard analysis shall be performed on software containing safety-critical functions. The effects of command input timing and of processor timing shall be included in the analysis.

All software requirements, designs, code modules, interfaces, and tests which are identified as safety-critical shall be documented and placed under configuration control. Any flight software identified as safety-critical shall be placed in the software classification as designated by the project in its SeaWinds Instrument Software Management Requirements (PD 686-014). Safety-critical software shall be subject to the same development procedures, constraints, documentation requirements, reviews, inspections, configuration management,

change control, and problem/failure reporting requirements as all other high-level non-safety-critical flight software.

Waivers of software safety requirements shall meet all the procedures for hardware safety requirement waivers.

2.7 ELECTROEXPLOSIVE SYSTEMS

The following requirements govern the basic design requirements for electroexplosive ordnance devices. Unless specified otherwise by an outside agency, the requirements of MIL-STD 1576 shall be met.

2.7.1 Classification

Electroexplosive ordnance devices shall be classified as either Category A or Category B. SeaWinds' policy is to design all circuitry, harness, and mechanical equipment in the same manner as Category A.

2.7.2 Safe and Arm Devices

Safe and arm devices shall meet the requirements of MIL-STD 1576.

2.7.3 Device Mechanical Design

2.7.3.1 Impact and Friction Sensitivity. The explosive material used in Category A devices shall have an impact sensitivity not greater than lead styphenate, and a friction sensitivity no greater than lead azide.

2.7.3.2 Drop Tests. Category A and B devices shall not detonate or ignite when dropped a distance of 1.8 meters onto concrete in the most susceptible orientation.

2.7.3.3 Shipping and Handling. Devices shall withstand the vibration effects of shipping and handling without ignition or detonation, and shall function properly after subjection to vibration testing.

2.7.4 Device Electrical Design

2.7.4.1 Initiators. Electroexplosive devices shall meet the requirements of MIL-STD 1576. The NASA Standard Initiator meets the MIL-STD 1576 requirements.

2.7.4.2 Electrical Connector. Electroexplosive devices shall contain an electrical connector, integral to the unit, so that the device can be connected and disconnected electrically from the firing circuits.

2.7.4.3 No-Fire Current/Power. Category A devices shall not initiate or deteriorate in performance when one ampere direct current and one watt power minimum are applied to the device for a minimum of five minutes.

2.7.4.4 Electrostatic Discharge Protection.

2.7.4.4.1 Shielding Caps. Electroexplosive devices shall have shielding caps installed which meet the following requirements:

(1) The outer shells shall be made of conductive material.

(2) The outer shell shall make electrical contact with the device case.

(3) No gaps shall exist between the shielding cap and the case.

(4) The cap shall not contact the pins.

2.7.4.4.2 Bleed Resistors. Electroexplosive devices shall be protected from electrostatic hazards by the placement of resistances from line-to-line and from line-to-ground (structure) as appropriate. The placement of line-to-structure static bleed resistances is not considered to violate the single-point ground requirements as long as they are 10k ohms or more.

2.7.4.4.3 Electrostatic Discharge Test. Electroexplosive devices shall meet the electrostatic discharge test as required in MIL-STD 1576.

2.7.5 Circuit Design

MIL-STD 1576 shall be followed for the circuit design for all electroexplosive systems (Category A or B).

2.7.6 Identification

Electroexplosive devices shall be color coded to indicate the explosive condition of the specific item. The color coding may be satisfied by the attachment of a permanent label of the appropriate color (as follows) with the simulator type, part number, and serial number listed:

(1) Live explosive: Natural.

(2) Inert-dummy model: Yellow.

(3) Inert-resistance simulator: Green.*

(4) Inert-bridgewire simulator: Blue.*

* Color coding of simulators is not required if the device is designed such that installation into the pyro device is not possible.

[--- Unable To Translate Graphic ---]

SECTION 3

GROUND SUPPORT EQUIPMENT DESIGN REQUIREMENTS

3.1 GENERAL

Ground Support Equipment shall be designed in accordance with the requirements established in this section.

3.1.1 Explosion-Proofing

Explosion-proof connectors and equipment shall be used for circuits which can potentially be energized when an explosive environment either exists, or could exist in the event of a mishap. Circuits which are intrinsically safe by virtue of their low voltage and current levels need not be explosion proof.

3.1.1.1 Use With Flammables. Equipment intended for use with flammable solids, liquids, or gases shall be designed and fabricated using equipment with an explosion-proof rating.

3.1.1.2 Use in Potentially Explosive Environments. For equipment which is only incidentally employed in potentially explosive environments, the following techniques shall be employed to render the equipment hazard-proof. Techniques other than using explosion-proof-rated equipment shall be approved by the JPL Safety Oganization and by the appropriate outside safety organization if the equipment is used at a site other than JPL. The techniques are listed in order of preference:

(1) Hermetically sealing or potting.

(2) Inert gas purging.

(3) Inserting in an enclosure with a continuously supplied inert gas.

(4) Selective operation by a local attendant/operator only when an explosive atmosphere is verified not to exist. This method requires continuous presence by the attendant/operator and the ability to power-down the equipment with a single switch or power disconnect.

3.1.2 Fault Tolerance

Ground Support Equipment, including equipment for test and evaluation which is not formally delivered to the project, as a minimum, shall be designed to preclude damage to the flight equipment in the event of a single failure in the support equipment.

3.1.3 Computer Controls

GSE that employs computerized/software controls of potentially hazardous activities shall explicitly define control functions in documentation of a step-by-step basis to the level of detail such that each function can be reviewed and any potentially hazardous states can be identified. Emergency flags shall be written in safing or shutdown procedures. All personnel operating the equipment during hazardous activities shall receive training on these procedures.

Computer software controls of hazardous GSE functions shall be evaluated for fault tolerance and designed for appropriate control. This includes situations where multiple software controls are used but are implemented on the same hardware, or software controls are employed on different hardware platforms which have a common single-point failure such as all hardware being connected to the same electrical power source. Backup mechanical or manual emergency safing functions shall be available. (See Section 3.6 for additional software safety requirements for GSE.)

3.2 MATERIALS

3.2.1 Stress Corrosion

Materials resistant to stress corrosion shall be used in GSE which may be in contact with or provide support for SCI's.

3.2.2 Flammability

Materials used in the manufacture, assembly, test, and packaging of essential electronic equipment shall be flame retardant under all conditions to which the equipment will be exposed. SeaWinds Critical Items (especially electronic equipment) and equipment shall make the maximum practicable use of nonflammable, fire-proof, fire-resistant, and fire-retardant materials.

3.3 MECHANICAL SUPPORT EQUIPMENT

3.3.1 Design Load Factors

The load factors which are summarized in Table 3.1 below shall be used in the design and analysis of ground equipment (cranes, ground support equipment, fixtures, handling equipment, or shipping and transportation equipment, etc...) used for handling flight equipment. The ground equipment shall be tested. During proof-test, the test load shall be applied along a line which would go through the center of gravity of the SCI which the equipment was intended to support.

Table 3.1
Minimum GSE Design Load Factors

	Vertical Direction		Lateral Direction[1]	
Material	Ult	Yld[2]	Ult	Yld
Rope Slings:				
Nylon, polyester rope	18	--	--	--
Polypropylene rope	12	--	--	--
Web Slings:	5	--	--	--
All Other Materials[2]	5	3.75	0.63	0.47[3]

[1]Times vertical-rated load. Assumes maximum of 0.25 g on the vertical-rated load for lateral (side) load. If greater lateral loads are possible, a factor of 2.5 ultimate and 1.875 yield x expected side load must be used.

[2]The GSE must be designed such that general yielding does not occur when proof-tested to 3.5 x rated load.

[3]Side-load factor (0.25) times yield safety factor (1.875) on the lifted weight.

3.3.2 Hook Safety Latches

The lifting hooks of cranes or other lifting equipment used to lift a SCI shall be equipped with safety latches.

3.3.3 Handling and Lifting Fixtures

The following structural considerations shall be employed in the design of SCI fixtures or handling equipment:

(Note: Qualification by test without a supporting analysis is acceptable.)

(1) Structural strength shall be adequate to sustain the static and dynamic loads applied to the fixture or equipment under worst case conditions.

(2) Structural stiffness shall be adequate to prevent deformation which might induce unwanted local loads into the flight equipment structure or which might compromise the functional ability of the fixture or equipment during all expected environments.

(3) Lifting fixture overturning moments and stability, proof load, and center of gravity constraints shall be analyzed.

(4) Natural fiber rope shall not be used in fixtures to be used with SCI.

3.3.4 Storage, Shipping, and Transportation Equipment

Containers for two situations are addressed in this section:

3.3.4.1 Fabrication and Local Storage. The following design criteria as a minimum shall apply to fabrication fixtures and storage containers used for SeaWinds Critical Items:

(1) Shock and vibration dampening devices shall be incorporated if the hardware could be damaged by these environments.

(2) Shock and vibration monitoring devices shall be incorporated into the container, if the hardware is sensitive to these environments.

(3) A moisture seal shall be incorporated if the hardware could be damaged or degraded by exposure to the ambient environment and is not otherwise protected against moisture.

(4) Internal attachment devices/features, incorporated as an integral part of the container design, shall be provided to the maximum extent practicable.

(5) If the equipment is moisture sensitive, a desiccant chamber, or other drying medium, shall be exposed to all equipment voids.

(6) Insulating materials for protection against excessive heat shall be flame resistant and appropriate for the degree of protection required by the particular equipment.

(7) Materials used in the fixtures and containers shall not be susceptible to electrostatic charge build-up if the hardware is ESD sensitive, or if the fixture/container is used to transport the hardware into ESD-controlled areas.

(8) Metal surfaces shall be protected against environmental or galvanic corrosion.

(9) There shall be no sharp points or burred edges which could cause injury to personnel or damage to the hardware.

(10) Materials shall not outgas or otherwise contaminate the hardware. This must

be considered even if the specific hardware is not sensitive to the contamination.

(11) Specific consideration shall be given in the container design to preclude blocking container hardware vents or breathers (i.e. battery vent caps).

3.3.4.2 Transportation. The following requirements shall be applied to containers used for transportation of SeaWinds Critical Items:

(1) The container shall be available for use in the first and all subsequent shipments of SCI's.

(2) The design shall permit safe packing and unpacking without functional damage to the fixture or the equipment itself.

(3) The size, shape, and weight of the container shall be consistent with the requirements of the intended mode of transportation.

(4) The structural materials shall be resistant to impact, fire, and stress. Reinforced plastics are acceptable if precautions are taken to prevent electrostatic buildup and contamination. Outgassing properties of the materials shall be considered in their selection.

(5) Container materials shall be resistant to oil and water absorption.

(6) Container materials and surfaces shall be easy to clean. The container shall be as light in weight as safety factors and practicability permit consistent with hardware protection requirements.

(7) Metal surfaces shall be protected against galvanic and environmental corrosion.

(8) The container shall have no sharp points or burred edges that could cause injury to personnel or damage to hardware.

(9) Shock absorbing or vibration damping devices or material shall be used to protect delicate or sensitive equipment. Monitoring devices shall be included for particularly sensitive equipment. The weight vs. drop-height requirements in Table 3.2 shall be used for test/analysis of the container design.

(10) Gripping devices or handles shall be firmly fastened to the container to facilitate ground handling. Fixed hoisting or fork-lifting attachments, when required, shall form an integral part of the container design.

(11) Sealed containers shall have a pressure release system. Operating instructions shall be posted conspicuously on the outside of the container. As a minimum, the design of a sealed system shall have a safety factor of 4 on ultimate stress under all conditions that might be encountered. Containers which will be exposed to differential pressures exceeding 103.4 kPa (15 psi) shall require specific approval of the design by the JPL Safety Oganization.

(12) Packaging materials such as "bubble wrap" shall be verified as non static chargeable and shall not exert excessive force on flight hardware due to expansion throughout the expected pressure range of the transportation environment.

(13) All flammable containers shall be protected with fire-retardant paint.

[--- Unable To Translate Graphic ---]
[--- Unable To Translate Graphic ---]

Table 3.2

Container Weight and Drop Height
[--- Unable To Translate Graphic ---]

Total Weight (Including Package)		Acceptable Limits		
		Drop Height		Load Factor
Kg	(lbs)	(cm)	(inches)	(g)

[--- Unable To Translate Graphic ---]

0 - 9.3	(0-20)	107	(42)	< 30
9.3 - 22.9	(21-50)	91	(36)	< 30
22.9 - 113.6	(51-250)	76	(30)	< 30
113.6 - 227.0	(251-500)	61	(24)	< 30
227.0 - Up	(501-up)	46	(18)	< 30

[--- Unable To Translate Graphic ---]

[--- Unable To Translate Graphic ---]

3.3.4.3 Container Identification. The shipping containers for all SCI's shall be identified with shipping instructions and distinctive markings as follows.

NOTE

This requirement can only be exempted when the system-level shipping containers (spacecraft) are escorted at all times during movement.

3.3.4.3.1 Instructions. A transparent plastic envelope shall be attached to one of the four vertical sides of each shipping container. The envelope shall contain a card with the word "EMPTY" printed on one side and the following information on the other (see Section 3.3.4.1(7) for ESD concerns).

(1) Notification of ownership.
(2) Destination.

(3) Who may open the container.

(4) Temperature limits.

(5) Humidity restrictions for opening.

(6) Shock or vibration level limitations.

(7) Any time-critical factors.

(8) Any hazardous materials notifications, limitations, identifications, etc.

(9) Ionizing/non-ionizing radiation restrictions.

When a container is empty, the reversible card shall be turned so that the word "EMPTY" is displayed.

NOTE

Containers with hazardous materials shall be identified and comply with design and handling requirements of the appropriate DOT regulation.

3.3.4.3.2 Distinctive Markings. Containers for SCI's shall have the four top corners painted on the outside of the container with solid bright international orange. The extent of the triangular shaped area at each of the top corners shall be as follows (see Figure 3-1):

(1) Locate a point 15 cm (6 in) along each of the converging edges.

(2) The total area bounded by the three points shall be solidly painted.

(3) For odd shaped containers (e.g. spherical or cylindrical), the equivalent diamond-shaped marking shall be applied.

(4) The empty and loaded weight shall be clearly posted on all containers that weigh more than 23 kg (50 lb).

(5) The words "FLIGHT HARDWARE" or "PROJECT-CRITICAL HARDWARE" shall be conspicuously displayed on each of the four vertical sides of the container.

(6) The proper and acceptable orientation of the container shall be identified with "THIS SIDE UP," "TOP," "UPRIGHT," or other appropriate unambiguous markings.

Figure 3-1. Flight Equipment Container Markings

3.4 TEST EQUIPMENT

Commercial and special test equipment, whether used individually or integrated into an equipment rack containing several pieces of test equipment, shall conform to the following requirements.

3.4.1 Connectors

3.4.1.1 Connector Savers. Connector savers shall be attached to SCI connectors at the earliest opportunity. The connector saver shall consist of a flight quality connector which mates with the SCI, a short length of cable and a "workhorse" connector which will mate with the non-SCI.

3.4.1.2 Connector Keying. Multi-pin connectors supplying power or signals to any part of the flight equipment shall be sized and/or keyed to prevent incorrect insertion or connection of wrong connectors. Mechanical and electrical analysis shall be performed to eliminate any possible misconnection.

3.4.2 Racks

Each test equipment rack shall employ transformer isolation between the facility power mains and all equipment within the rack. The secondary of all power isolation transformers shall be referenced to ground.

3.5 RADIATION

3.5.1 General

Ground Support Equipment which emits either ionizing or nonionizing radiation and which interface with radiation-emitting hardware shall be designed to minimize the release of radiation to the environment and personnel.

Ground Support Equipment and test equipment which emits any form of harmful nonionizing radiation at potentially harmful levels shall be reviewed and approved by the JPL Safety Organization.

3.5.2 Placarding

Ground Support Equipment whose radiation could be harmful shall have warning placards conspicuously attached to the equipment. The following information shall, as a minimum, be included on the placard: (1) Type of radiation; (2) Field strength or intensity as a function of distance from the equipment; and (3) Personnel exposure limitations.

3.6 SOFTWARE

3.6.1 Inhibits

Safety-critical functions shall include noncomputer-controlled inhibits which will preclude the inadvertent occurrence or command of that function in the event of a computer hardware or software failure.

3.6.2 Hazard Analysis

A Software Hazard Analysis shall be performed on software containing safety-critical functions. The effects of command, input, and processor timing shall be included in the analysis.

3.6.3 Displays

Systems containing data displays which, if displaying erroneous data, could cause an operator to take action which could be harmful to flight equipment or hazardous to personnel shall be subjected to a hazard analysis (Section 3.6.2).

SECTION 4

TEST AND OPERATIONS REQUIREMENTS
[--- Unable To Translate Graphic ---]

4.1 GENERAL

4.1.1 Applicability

The requirements of Section 4 shall apply to SeaWinds Critical Item (SCI) operations at all levels of assembly, at JPL and non-JPL facilities.

Since there are limited spares, some GSE including piece-parts and components become project-critical.

NOTE

> The requirements for GSE computer controls and for GSE software which are stated in Section 3.1.3 and 3.6 of this document are also applicable to test, handling, assembly, transportation, and other project-critical equipment, facilities, and operations.

4.1.2 Notification

The Hardware or the Test and Operations Cognizant Engineer shall notify the SeaWinds Systems Safety Engineer sufficiently in advance of all flight hardware transportation or hazardous test activities to permit SeaWinds Systems Safety Engineer attendance at planning meetings and reviews.

4.1.3 Proof-Testing and Validation of Handling Equipment

Equipment involved in the handling and transportation of flight hardware shall be inspected and tested per the requirements of the following sections.

4.1.3.1 Frequency. A thorough checkout of SCI handling equipment, including evidence of proof testing, shall be made within two weeks of the start of the flight hardware handling operation.

The checkout period is extended to a maximum of six months prior to operations if the equipment is maintained in a controlled area where it is protected from undesirable environments and unauthorized use.

This checkout shall be repeated at least every six months for equipment which is subject to excessive wear or damage and at least annually otherwise.

4.1.3.2 Inspection. A copy of the inspection report or P/FR identifying discrepancies discovered during inspection after the equipment is placed into initial service, and the corrective action, shall be forwarded to the SeaWinds Systems Safety Engineer.

4.1.3.3 Reporting. Checkout or testing information generated in evaluating equipment for SCI handling shall be recorded and retained until the equipment is destroyed, surplused, or otherwise disposed of.

4.1.3.4 Placards. The support equipment rated load, date of proof-test and date of next re-proof test shall be indicated on a tag (JPL Drawing No. 10025963-1 or equivalent) conveniently and conspicuously attached to the support equipment.

4.1.3.5 Cranes.

4.1.3.5.1 Frequency. Cranes shall be inspected and proof-tested immediately prior to use with SCI's and annually thereafter. Cranes and other lifting devices or equipment attached to a facility shall be carefully checked for potential damage prior to use after an earthquake. Attachment points to the facility, rail straightness, and bridge/trolley rollers or wheels shall receive careful inspection.

4.1.3.5.2 Proof-Test Factors. Cranes used for handling SCI's shall be proof-tested to the test factors as follows:

1.75 x SCI weight x realistic dynamic factor.

If the realistic dynamic factor is unknown, a factor of 2.0 shall be assumed, yielding an overall factor of 3.5.

If the realistic dynamic factor is known to be less than 1.25, then 1.25 as a minimum shall be used, yielding an overall factor of at least 2.2.

In no case shall the proof-load exceed the crane manufacturer's operating load rating x 1.25.

4.1.3.5.3 Method. Cranes and lifting equipment shall be proof-loaded and, as a minimum, tested as follows:

(1) Visual inspection.

(2) Dynamic tests of lifting and braking mechanisms at maximum possible speeds.

(3) Traversing the entire travel in all directions with the proof-load attached.

4.1.3.5.4 Placards. Placards indicating the maximum SCI weight to be lifted by the crane shall be placed on the control pendant/panel. The placard shall be worded so that the maximum allowable SCI weight cannot be confused with the crane manufacturer's rating.

4.1.3.6 Assembly and Handling Support Equipment. The following loads shall be applied at, or through, the center of gravity of the item being tested.

4.1.3.6.1 Proof-Test Factors. SCI hardware handling equipment shall be static-tested using the following factors (see Figures 4-1 and 4-2):

1.75 x SCI hardware weight x realistic dynamic factor.

If the realistic dynamic factor is unknown, a factor of 2.0 shall be assumed, yielding an overall factor of 3.5.

If the realistic dynamic factor is known to be less than 1.25, then 1.25 as a minimum shall be used, yielding an overall factor of at least 2.2. Where the 2.2 proofload factor is used, the proof load should be done in a dynamic fashion such as lifting and traversing the proof load on the cranes or other rotational/positioning devices at the highest speed as opposed to the slowest speed as would be done for a static test.

4.1.3.6.2 Side-Load Test Factors. Handling equipment which may at any time receive side loads shall be tested for side loads (horizontal direction). The side load for test shall be 0.25 times the dynamic proof-test load (0.44 times the SCI equipment rated load).

The side load shall be applied simultaneously with the vertical proof-test load.

4.1.3.7 Miscellaneous Equipment.

4.1.3.7.1 Hydra-Sets. Hydra-sets shall meet the same annual proof-load testing criteria applied to all other JPL lifting and handling equipment.

Hydra-Sets are to be mechanically proof-load tested to 2.0 times the full scale load rating with the piston bottomed out. Since this does not meet the JPL maximum "g" proof-load requirement of 3.5, the Hydra-Set shall be derated to 2.0/3.5 = .57.

In addition to mechanical proof testing, the hydraulic circuits shall be proof tested to demonstrate safety margin in the hydraulic fluid system. If the maximum hydraulic proof test performed is at the Hydra-Set full scale rating (100%), the hydra-set shall be de-rated to a maximum rating or 1.0/1.5 = .67.

The maximum load allowable shall be based on the lower of the mechanical and hydraulic factors. Without any special analysis or testing above rated load, the maximum allowable hardware load shall be .57 times the full-scale rating of the Hydra-Set.

Figure 4-1. Static Proof Testing

Figure 4-2. Dynamic Proof Testing

Hydra-Sets shall never be loaded beyond the full-scale load rating while the piston is not fully extended. (Refer to Section 4.2.2.3 for use.)

4.1.3.7.2 Load Cells. Load cells shall be annually proof-tested to the maximum load recommended by the manufacturer. When the proof test load using the factors of Paragraph 4.1.3.6.1 exceed the manufacturer's recommendations, then the load cell shall be tested to the manufacturers maximum level and shall be derated for SCI use by using the formula: Max Load = [(1+ max. % load applied)/1.75 x accel. load factor] x load cell rating. Load cells shall be calibrated after each proof test.

4.1.3.8 Location. Proof-testing of cranes or equipment shall be performed in a location which precludes possible SCI damage in the event of a failure. If crane or equipment proof-tests cannot be performed as required due to the presence of flight hardware, a Systems Safety Request for Waiver shall be submitted to the JPL Safety Organization.

4.1.4 Test and Servicing Equipment Proof and Validation

Electronic GSE and test instrumentation shall be initially validated and/or calibrated before use and at predetermined intervals thereafter. The calibration due date shall be posted on the equipment.

4.1.5 Procedures

4.1.5.1 Required Use. The following types of operations shall be performed using approved and reviewed procedures:

(1) Operations involving SeaWinds Critical Items.

(2) Support equipment validation or qualification tests.

(3) Hazardous operations.

4.1.5.2 Marking of Cover. Procedures shall be marked on the front cover with one of the following statements:

(1) "THIS PROCEDURE CONTAINS HAZARDOUS OPERATIONS" (to be stamped in bold RED letters).

(2) "THIS PROCEDURE DOES NOT CONTAIN HAZARDOUS OPERATIONS" (to be stamped in bold BLACK letters).

4.1.5.3 Caution Notes. A caution note shall appear in the procedure immediately prior to a step which could be hazardous to equipment.

4.1.5.4 Warning Notes. A warning note shall appear in the procedure immediately prior to a step which could be hazardous to personnel.

4.1.5.5 Hazardous Commands. A hazardous command list or matrix shall be developed showing each major test configuration and identifying the specific commands which require special inhibits, warnings, or other precautions prior to issuance of the command. The method of control of the hazardous command shall be identified.

4.2 TRANSPORTATION AND HANDLING

4.2.1 General Handling

4.2.1.1 Responsibility. The handling and movement of delicate, critical, costly, or hazardous items shall be done under the control of the hardware cognizant engineer to ensure that safety of both personnel and hardware are fully maintained.

4.2.1.2 Buddy System. Two or more persons shall always be involved in the handling and movement of SCI's. At least one of these persons shall be knowledgeable of, or directly associated with, the equipment being moved. Also at least one of these persons shall be tasked with observing for hazards during movement, opening doors, controlling pedestrian or vehicular traffic, etc.

NOTE

Where flight hardware is small and light enough to be easily carried by one person (e.g., when transporting small flight items by plane or car), judgment may be made for practical and economic reasons.

4.2.1.3 Untrained Personnel. Untrained personnel involved in the handling or movement of a SCI shall be escorted by trained personnel with flight hardware certification. Such personnel shall be specifically briefed with instructions and precautions appropriate to the specific hardware involved.

4.2.1.4 Grounding. Personnel and equipment grounding requirements shall be observed during movement of ESD-vulnerable SCI's to prevent the accumulation of electrical charges.

4.2.1.5 Procedures and Instructions. Specific written instructions or procedures shall be issued for packaging, handling, shipping, and safeguarding SCI's. These instructions shall cover known contingencies, including:

(1) Periods when the equipment is not under the direct control of the furnishing technical cognizant organization.

(2) Periods when such equipment is to be transported, shipped, tested, stored, or used in areas over which the furnishing organization does not have complete control.

(3) Periods when such equipment is in a facility where a cognizant engineer is not in constant attendance.

It shall be the responsibility of the cognizant technical Manager to verify that the generation of proper transportation and handling instructions or procedures is accomplished.

4.2.1.6 Storage. Whenever assembly, inspection, and test operations are not being performed on the SCI, it shall be kept in designated areas that will protect the equipment from damage due to accident or earthquake.

4.2.1.7 Falling Objects. Suitable overhead protective coverage shall be provided when assembly, inspection, and test operations are conducted in areas where overhead objects could fall on the SCI, especially during earthquakes.

4.2.1.8 Work Surfaces. The following requirements shall be observed for work surfaces to protect hardware during work activities and earthquakes:

(1) Assembly, inspection, or test benches shall have nonskid surfaces and, to the maximum extent practicable, shall have strong lips or rims to prevent hardware from rolling or sliding to the floor.

(2) Special holding fixtures shall be used to firmly attach equipment to the work surface for assembly, inspection, and test operations whenever such attachment is practicable.

(3) Work surfaces shall incorporate ESD protection as defined in Section 4.2.4, if the equipment activity or the area control requires such protection.

4.2.1.9 Handling Equipment. The Cognizant Hardware Engineer shall verify that all handling equipment used for SCI's is:

(1) Operated by certified personnel.

(2) Operating safely.

(3) Suitable for the task.

(4) Qualified for the task (inspected, proof-tested, certified, etc.).

(5) Used in a proper and safe manner.

(6) Clean and uncluttered, with no objects present that could roll or fall against an item.

4.2.2 Lifting Operations

4.2.2.1 Cranes. The following requirements for utilizing cranes and hoists for SCI's shall be observed.

4.2.2.1.1 Emergency Shut-off. The emergency shut-off power breaker or switch shall be manned at all times that the crane is energized and attached to a SCI. A communication path between the crane operator and the person attending the emergency shut-off device shall be established and verified prior to the initiation of the lifting operation.

4.2.2.1.2 Suspended Equipment. SCI's shall not be left suspended or hanging unattended on cranes or other lifting devices for extended periods of time.

Under no circumstances shall personnel be allowed under a suspended load without appropriate supports. In order to enter the area under a suspended load, stable supports shall first be positioned in such a manner that should the load fall, it would fall onto the supports which shall be of sufficient height and stability that the personnel under the load would not be injured.

4.2.2.1.3 Umbrellas. Overhead lifting devices, including cranes and cherry pickers, shall include a protective shield, tray, or parasol or umbrella to protect the SCI from overhead debris or lubrication drips which may fall from the overhead apparatus.

4.2.2.1.4 Restricted Motion. Movement of cranes and other lifting devices shall be restricted to a single direction of movement when within 1.5 meters (5 feet) of a SCI.

4.2.2.1.5 Side Loads. Side loads shall not be allowed on a crane, hook, or cable at any time with or without a load on the hook.

4.2.2.2 Proof-Loading. The proof-load status of the crane and all lifting equipment shall be verified to be current prior to the lifting operation (refer to Sections 4.1.3.5, Cranes, 4.1.3.6, Assembly and Handling Support Equipment, and 4.1.3.7, Miscellaneous Equipment).

4.2.2.3 Hydra-Sets. Manually controlled Hydra-Sets, or cranes with inching motors, shall be utilized when mating or demating sensitive hardware joints during lifting operations. The following requirements shall be observed when using Hydra-Sets. (Refer to Section 4.1.3.7.1 for proof test requirements.)

4.2.2.3.1 Pneumatically Controlled Hydra-Sets. Pneumatically controlled "Hydra-Sets" shall not be used for handling SCI's.

4.2.2.3.2 Load Measuring Device. When the neutral-mass lift point must be known during a mating or demating operation, a load measuring device (load cell, etc.) shall be included in the lifting equipment.

4.2.2.4 Tag Lines. Equipment that will be lifted higher than a comfortable personnel reach shall be controlled by the use of sufficient tag lines to prevent unwanted rotation or swinging.

4.2.2.5 Fork Lifts. The overturning moment of the fork lift, including the flight equipment load, shall not exceed 50 percent of the fork lift maximum allowable overturning moment.

4.2.3 Transportation Between Sites

"Between sites" is defined as movement or transportation outside facility or institution boundaries requiring movement over public roads or highways, or other means not under the total control of the hardware cognizant organization.

4.2.3.1 General. Flight equipment shall be enclosed in special containers to protect the equipment against physical, environmental, and static charge damage while being transported.

4.2.3.2 Environmental Loads. The shipping and transportation induced environment at the SCI /fixture interface, or at the center of gravity of the assembly or its subsystem, shall at no time exceed a defined fraction of the allowable design load. Transient or peak loads which may exceed a total of 2g (1+1g) on the GSE fixtures shall be specifically considered in determining the GSE proof load requirements defined in Section 3.3.1.

The cumulative fatigue level of the SCI and its transporter experienced during shipping and transportation shall not exceed the predetermined values. These values are a function of the structural design of the SCI and its transporter and shall be determined by the Cognizant Structural Engineer.

4.2.3.3 Container Qualification. The containers used for the transportation of flight equipment shall be designed, qualified, and identified in accordance with the requirements of Section 3.3.4.

4.2.3.4 Separation of SCI & Non-SCI Units. Non-SCI shall not be shipped in the same container as the SCI.

SCI's may be shipped in groups within a single qualified container if properly packed and if loss of the container would not seriously impact the project.

4.2.3.5 Separation of SCI Hardware. SCI hardware shipments shall be separated and divided such that the complete loss of a shipment shall not cause the loss of a program (This requirement does not apply to the shipment of a one and only system or subsystem). This requirement should be interpreted as follows:

(1) Primary and spare hardware should be shipped separately.

(2) If a full complement of spares does not exist, then prime and redundant elements of the flight complement of hardware should be shipped separately.

4.2.3.6 Evaluation of Environments. Containers and transportation equipment used to ship large assemblies, subsystems, or systems shall be subjected to evaluation test runs in the air or on the

ground to evaluate and verify the acceptability of the actual magnetic, shock and vibration environments.

4.2.3.7 Highway Movements. The following requirements shall be observed when moving large SCI assemblies over the highway:

(1) The truck or highway van to be used shall be visually inspected for defects such as suspension system structure and mechanism, misalignment, tire wear, tie-down fixtures, etc. This inspection shall be performed prior to loading the SCI, and daily while en route.

(2) Once qualified, the truck or highway van shall not be used for any other activities prior to transporting the flight hardware.

(3) Triaxial accelerometers shall be installed on the van floor at each of the SCI mounting locations exactly as was previously done during evaluation and qualification.

(4) Outputs of all accelerometers shall be continuously recorded on magnetic tape or other permanent recording equipment throughout the trip.

(5) A warning system shall warn the driver when acceleration levels predetermined by the environmental requirements engineer are exceeded.

(6) If the warning system is triggered or a high-level acceleration environment is suspected, the van shall be stopped immediately and the cause investigated.

(7) Personnel familiar with all phases of the instrumentation and data recording system shall accompany the van.

(8) The speed of the truck shall never exceed 88 kilometers per hour (55 miles per hour).

4.2.3.8 Aircraft Movements. All practicable means shall be employed to evaluate the air transportation environment. Actual tests using flight model simulators may be impractical due to equipment availability and cost. An analytical evaluation may be made if sufficient aircraft dynamic characteristics are accurately known.

4.2.3.9 Safety Review. Transportation of SCI hardware at the subsystem level or above shall be preceded by a Transportation Safety Review as detailed in 4.7.3.

4.2.4 Electrostatic Discharge

The presence of static electricity at levels sufficient to destroy or cause latent damage to sensitive components cannot be detected or determined by human senses.

An electrostatic discharge control plan shall be generated by each Contractor. The plan shall show the implementation to reduce static charges to an absolute minimum to avoid damage to sensitive components.

The relative humidity shall be 30% or more anytime work is performed on ESD sensitive items.

4.2.5 Pyrotechnic Devices

4.2.5.1 Packaging. Pyrotechnic devices shall be packaged in and protected by a conductive material approved by the Safety Officer of the facility or installation where the devices are located. The packaging shall comply with all state and DOT regulations.

4.2.5.2 Transportation. Shipments of pyrotechnic devices shall comply with municipal and state regulations.

4.2.5.3 Shielding Caps. Electroexplosive devices shall have shielding caps installed at all times that the device is not cabled to either flight or test equipment.

4.2.5.4 Personnel Protective Equipment. Personnel involved with the inspection, handling, or test of pyrotechnics shall utilize protective equipment.

4.2.5.5 Electroexplosive Device Connection. Stray voltage checks shall be made before installing electroexplosive devices into their receptacles.

4.2.5.6 Electronic Equipment. Electronic equipment associated with the system and powered by the facility supply shall not be used in checkout during the pyrotechnic installation.

4.2.5.7 Procedures. Inspection, assembly, test, and installation activities or operations shall be performed using approved, released procedures. These procedures shall include emergency and contingency procedures, as well as standard operating procedures for the specific facility or area in which the work is taking place.

4.2.5.8 Grounding and ESD. Electrostatic discharge shall be controlled by dissipating the charges to ground as fast as they are generated.

4.2.5.9 Records Review. Transportation, storage, and handling records shall be reviewed to determine if environmental conditions (thermal, shock, humidity, vibration) could have degraded the pyrotechnic devices.

4.3 FACILITIES

4.3.1 Reviews

A review of all facilities used in the assembly, test, or evaluation of SCI's shall be conducted per Section 4.7.1. Among items covered will be the definition of the scope of

activities within the facility, including a list of all operations and modes planned involving the hardware.

4.3.2 General Facility Practices

In facilities used for the assembly, inspection, or test of flight equipment, precautions shall be taken to protect SCI's from the potential of damage due to broken or leaking overhead fluid systems or normal/accidental discharge of automatic sprinkler systems.

4.3.3 Clean Rooms

Clean rooms are designed to protect the flight hardware from the local ambient environment and shall be designed and operated in accordance with Federal Standard 209 or equivalent. A plan shall be written and followed to protect the hardware from damage caused by the clean room itself.

4.3.4 Fire Protection

In case of fire on or near the flight equipment, Halon extinguishers shall be used as the first choice of extinguishing agent unless other types are specifically required due to the presence of unique materials requiring other agents.

4.3.5 Lightning Protection

For areas susceptible to lightning strikes, a plan must be established to maximize the protection to SCIs and personnel.

4.3.6 Earthquake Protection

If the Contractor's facilities are susceptible to earthquakes, a plan must be established to minimize the vulnerability of operations due to earthquakes and to protect SCIs and personnel to the maximum extent practicable.

4.4 NONIONIZING RADIATION

4.4.1 Microwaves

The allowable amount of radiation exposure to personnel at JPL or at off-site locations is:

(1) Less than 1 mW/cm^2 of continuous exposure in an 8 hour day and 40 hour week.

(2) From 1 mW/cm^2 and less than 10 mW/cm^2 of emergency exposure which shall be less than one hour in a 24 hour period.

A controlled area shall be established to prevent personnel from inadvertent exposure.

Radiation levels produced by equipment shall be quantitatively assessed to assure that personnel exposure limits are met.

4.4.2 Lasers

The area in which lasers are to be operated shall be approved by the Contractor's Safety Office. Access control shall be established to prevent nonoperating personnel from inadvertent exposure to the laser beam. Protection shall be provided to personnel in the area where lasers are being operated.

4.4.3 Ultraviolet Light

Personnel shall be provided with proper skin and eye protection when in the vicinity of ultraviolet equipment operating at levels greater than 0.1 mW/cm^2 for an eight-hour continuous exposure.

4.4.4 Ultrasonic Sound

Ultrasonic frequency sound generators shall be controlled and limited in the vicinity of the SCI or other sensitive hardware and personnel.

4.4.5 Audio Sound

Ambient noise levels shall be kept below 85 dB in areas where activities are being conducted without appropriate ear protection.

4.5 ELECTRICAL AND MECHANICAL TEST

4.5.1 Electrical Test Equipment

Test equipment to be connected to any SCI shall have the prior approval of each affected cognizant engineer before connection is made to ensure the compatibility of the internal circuitry with the electrical characteristics of the test equipment (e.g., grounding, impedance, voltage, or current).

4.5.2 Breakout Boxes

Breakout boxes shall be qualified (verified for proper circuit continuity and isolation) prior to use with SCI's.

4.5.3 Electrical Test Procedures

Electrical integration and test procedures shall provide for sufficient configuration

verification and continuity checks to assure that the circuitry is correct prior to the application of power to the circuit.

4.5.4 Hazardous Commands or Stimuli

Appropriate caution statements shall be included in the test procedures when conditions exist for the possibility of incorrect power or stimulus application, or the transmission of hazardous commands.

4.5.5 Connectors

4.5.5.1 Mating and Demating. Electrical connectors shall not be joined or separated when energized.

4.5.5.2 Inspection. Connectors shall be inspected for cleanliness and for pin alignment prior to each mating.
4.5.5.3 Authorization. The mating or demating of flight connectors shall be performed by specifically authorized personnel.

4.6 ENVIRONMENTAL TEST

4.6.1 Reviews

The Facility Safety Survey and the Operations Safety Survey specified in Section 4.7 shall be completed prior to the conduct of environmental test(s). An ESD survey shall be performed if necessary.

NOTE: To be Performed by JPL Personnel with Contractor support as designated.

4.6.2 Procedures

Environmental testing of SCI's shall be conducted in accordance with approved written procedures.

Changes to procedures shall be documented in writing prior to implementing the change and shall be approved by the original approval authority. Facility detailed test procedures and SCI functional test procedures shall define the specific contingency actions to be taken in the event of a test anomaly or malfunction.

4.6.3 Test Surveillance

An experienced, certified test facility operator(s) shall be in attendance at all times that the SCI is in test at conditions other than an ambient environment or in operation.

Operators shall understand the immediate contingency actions to be taken to return the test facility and flight hardware to a safe state in the event of a facility or test article malfunction.

4.6.4 Test Controls

4.6.4.1 Transducers. Control and monitor transducers used for acceptance testing shall be the same type, installed at the same locations, and interconnected in the same manner as those used for qualification or type approval testing of a like test article.

4.6.4.2 Calibration. Control and monitor transducers used for testing SCI's shall be in valid calibration status.

4.6.4.3 Overtest Protection. The test laboratory shall provide adequate protective devices for use during the tests to limit overtesting.

These overtest protective devices shall be independent of the normal automatic controlling devices. These protective devices shall be demonstrated to be operable prior to each test or test series.

4.6.4.4 Emergency Shutdown. Emergency shutdown buttons or switches shall be provided to permit dynamic tests to be immediately terminated by the test director and/or by specified observers.

The shutdown action shall not impose stresses or transients greater than originally planned to be imposed by the normal conduct of the test.

Electronic/computer controlled test equipment shall have a mechanical emergency shutdown capability in case of failure of electronic/computer controls.

4.6.4.5 Interlocks. Redundant monitors shall be provided which will remove power from the SCI in the event that unacceptable conditions can rapidly occur during test, e.g., instruments or electronics which can only be operated below certain vacuum or thermal levels.

4.6.5 Test Fixtures

Environmental test fixtures and adapters shall be verified by analysis and test for adequate fit and support of the SCI in the intended environments. The integrated facility/fixture combination shall be demonstrated to be capable of performing as expected over the entire environmental range to which it will be exposed during the SCI test.

4.7 REVIEWS/SURVEYS

NOTE: To be Conducted by JPL Personnel supported by Contractor Personnel.

The following surveys shall be conducted prior to the assembly, inspection, transportation, or test of SCI's. The surveys may be combined, provided that appropriate emphasis is given to each aspect of each individual survey. The level of formality of the process shall be as appropriate and necessary for the hardware and is determined using the applicability table in the survey checklist (To request a Survey(s), communicate with the contact at the address in the FOREWARD of this document).

The intention of the requirement to conduct Safety Surveys at JPL and at non-JPL facilities is to ensure the Manager fully understands all environments and operations to which his/her hardware will be exposed, and that all necessary and appropriate precautions have been implemented.

Attendees at the survey meetings at remote sites (non-JPL facilities) is a matter of judgement. The expertise represented by the named functions can be represented by fewer people. The nature of the activity determines the specific representation required.

4.7.1 Facility Safety Survey

A Facility Safety Survey shall be conducted for facilities used in the test or evaluation of SCI's.

4.7.1.1 Scheduling. Facility Safety Surveys shall be completed not more than two months prior to facility use for SCI activities. In scheduling the surveys, consideration shall be given to the urgency of the project schedule to assure that the survey is held with sufficient lead time to allow completion of action items which might be generated. Previous information from regular (annual or other) surveys can be taken into consideration to minimize repetition.

4.7.1.2 Attendees. As a minimum, attendees at the Facility Safety Survey shall include:

(1) Contractor hardware cognizant engineer.

(2) Contractor facility cognizant personnel.

(3) Contractor project representative. Hardware cognizant engineer may also act in this capacity.

(4) JPL Safety Organization representative.

(5) Contractor Safety Representative.

(6) Quality Assurance representative (JPL or Contractor).

(7) JPL Environmental Test Laboratory representative (for environmental tests).

4.7.2 Operations Safety Survey

A survey of the SCI and personnel readiness for the activity shall be conducted just prior to activities involving SCI's. The survey may cover a single activity, or a series of activities. It is recommended that the review be held at the site of the operation. In the case of continuing activities in a particular area, the survey shall be conducted at least once per year, or sooner if the scope of the activities changes.

4.7.2.1 Scheduling. The Operations Safety Survey shall be held when the facility, instrumentation, documentation, and cognizant personnel are ready for the activity.

4.7.2.2 Attendees. As a minimum, attendance of the following personnel shall be required at the Operations Safety Survey:

(1) Contractor hardware cognizant engineer.

(2) Contractor facility cognizant personnel.

(3) Contractor project representative. (Hardware cognizant engineer may serve in this capacity.)

(4) Quality Assurance representative.

(5) JPL Safety Oganization representative.

(6) Contractor Safety representative.

4.7.3 Transportation Safety Review

A Transportation Safety Review shall be conducted prior to the transportation of SCI's at the subsystem level or above. The review shall establish the adequacy of all handling and support equipment, lifting devices (including elevators, cranes, hoists, slings, etc.), containers, operations, precautions, vehicles, environments, instrumentation, procedures, and personnel qualifications to protect the item.

4.7.4 ESD Survey

An ESD survey shall be conducted in a facility whenever ESD vulnerable SCI's are being fabricated, tested or otherwise processed. The survey shall be repeated annually or sooner if significant modification is made to the facility or to the SCI and its test equipment.

4.8 PERSONNEL

4.8.1 Training and Certification

Personnel shall be trained and qualified for the operations and tasks which they are expected to perform on SCI's. The training and verification may be formal or informal, depending on the task and facility or field site requirements.

4.8.2 Extended Shifts

The work hours of personnel involved in the testing or operations of SCI's which are vulnerable to damage by operator or test operations error shall be limited. Due to the value and sensitivity of SCI's, steps shall be taken to guard against fatigue errors.

4.8.3 Operating Equipment Surveillance

SCI's shall not be left operating while unattended unless operating parameters and environment are stable and constant and if an "unattended" mode of operation which automatically removes power from the SCI in the event of abnormal SCI or environmental equipment performance is incorporated into the support equipment.

Where unattended operation is desired for long duration tests such as burn-in or other ambient environment activities, the cognizant Manager (or equivalent), shall specifically approve the test plan prior to the test.

4.8.4 Area Access

Personnel access to areas involved in SCI activities at all levels of fabrication, handling, transport, assembly, and test and operations shall be controlled.

APPENDIX A

PROOF TEST LABEL - AHSE